CLEARANCE-BASED METHOD FOR DYNAMICALLY CONFIGURING ENCRYPTION STRENGTH

FIELD OF THE INVENTION

The present invention relates to computer systems, and more particularly, to data access in computer systems.

BACKGROUND OF THE INVENTION

Certain computer systems in the industry require the encryption of data. For example, banking through the Internet typically requires a remote user to have a browser which supports the standard 128-bit SSL cipher suite for the encryption of data. However, with conventional systems, all of the data is either encrypted or not and with the same encryption strength. This is inflexible.

Accordingly, there exists a need for a method for dynamically configuring an encryption strength for data. The present invention addresses such a need.

SUMMARY OF THE INVENTION

The method for configuring encryption strengths for data includes: providing a piece of the data with a sensitivity level; authenticating a remote user with a clearance level for accessing the data; selecting an encryption strength for the piece of the data based on the clearance level of the remote user, if the clearance level of the remote user allows access to the piece of the data with the sensitivity level; encrypting the piece of the data; and providing access to the encrypted piece of the data to the remote user. Remote users have

varying levels of clearance to access data. Data is assigned varying sensitivity levels. Each clearance level allows the remote user to access data at that sensitivity level or below. The strength of the data encryption is based upon the remote user's clearance level or a requested session sensitivity level (a temporarily-lowered clearance that lasts as long as the current session). Access control to data is thus more flexible.

BRIEF DESCRIPTION OF THE FIGURES

Figure 1 illustrates a preferred embodiment of a system which utilizes the method for dynamically configuring an encryption strength for data in accordance with the present invention.

Figure 2 is a flowchart illustrating a preferred embodiment of the method for dynamically configuring an encryption strength for data in accordance with the present invention.

Figure 3 is a flowchart illustrating in more detail the preferred embodiment of the method for dynamically configuring an encryption strength for data in accordance with the present invention.

Figure 4 is a flowchart illustrating the method for dynamically configuring an encryption strength for data in accordance with the present invention, with the remote user requesting a session sensitivity level.

DETAILED DESCRIPTION

The present invention provides a method for dynamically configuring an encryption

strength for data. The following description is presented to enable one of ordinary skill in the art to make and use the invention and is provided in the context of a patent application and its requirements. Various modifications to the preferred embodiment will be readily apparent to those skilled in the art and the generic principles herein may be applied to other embodiments. Thus, the present invention is not intended to be limited to the embodiment shown but is to be accorded the widest scope consistent with the principles and features described herein.

The method in accordance with the present invention provides remote users with varying levels of clearance to access data. Data in the system is assigned varying sensitivity levels. Each level of clearance allows the remote user to access data of a certain sensitivity level and below. In the preferred embodiment, the sensitivity level of data is assigned by the local user. The "local user" is the user which owns the data. The "remote user" is the user who is seeking access to the data. "Sensitivity level" refers to a representation of the amount of damage that would be done to the local user if an unauthorized user gains access to the data. The remote user provides his clearance level for accessing data. Before the data is provided to the remote user, it is encrypted. The strength of the encryption of the data is based upon the remote user's clearance level or a requested session sensitivity level.

To more particularly describe the features of the present invention, please refer to Figures 1 through 4 in conjunction with the discussion below.

Figure 1 illustrates a preferred embodiment of a system which utilizes the method for dynamically configuring an encryption strength for data in accordance with the present invention. The system 100 includes an access and encryption software 102 which interfaces

with a piece of data 104, the remote user 106, and the local user 108. The remote user 106 has been assigned a clearance level, and the pieces of data 104 has been assigned a sensitivity level by the local user 108.

Figure 2 is a flowchart illustrating a preferred embodiment of the method for dynamically configuring an encryption strength for data in accordance with the present invention. First, a piece of data 104 with a sensitivity level is provided, via step 202. Next, the remote user is then authenticated, via step 204. Next, it is determined if the remote user 106 has clearance to access the piece of data 104. The piece of data 104 has been assigned a certain sensitivity level by the local user 108. If the remote user 106 does not have clearance to access the piece of data 104 of that sensitivity level, then access to the piece of data 104 is denied, via step 208. If the remote user 106 has clearance to access the piece of data 104 of that sensitivity level, then an encryption strength for the piece of data 104 is selected, via step 210. The encryption strength determines the cipher suite to be used. The piece of data 104 is encrypted with the cipher suite with the determined encryption strength, via step 212. The remote user 106 is then provided access to the encrypted piece of data, via step 214.

In the preferred embodiment, the encryption strength, and thus the cipher suite to be used, is based upon the remote user's clearance level. The local user 108 can configure the access and encryption software 102 to specify which cipher-suites are appropriate for each clearance level. For example, assume that the clearance levels range from "0" to "10", with "0" being the lowest clearance, i.e., access only to data intended for public consumption. The following is an example set of cipher suites assigned to the clearance levels:

- Level 0: no encryption, with 32-bit CRC error-detection

- Levels 1-3: 40-bit RC4, 40-bit RC2, or 56-bit DES, with HMAC
- Levels 4-7: 128-bit RC5, or 128-bit Blowfish, with RSA/MD5
- Levels 8-10: 3-key 3DES, or 256-bit Rijndael, with RSA/SHA1

Figure 3 is a flowchart illustrating in more detail the preferred embodiment of the method for dynamically configuring an encryption strength for data in accordance with the present invention. First, the remote user 106 sends his identification data, via step 302, which is then authenticated, via step 304. When the remote user 106 requests access to a piece of data 104 in the system 100, it is determined if the remote user 106 has clearance to access the piece of data 104, via step 306. If the remote user 106 does not have clearance to access the piece of data 104, then access to the piece of data 104 is blocked, via step 310. If the remote user 106 has clearance to access the piece of data 104, then an encryption strength for the piece of data 104 is selected based on the remote user's clearance level, via step 308. The piece of data 104 is then encrypted, via step 312, and access to the encrypted piece of data provided to the remote user 106, via step 314. Steps 306-314 are repeated for each piece of data to which the remote user 106 requests access.

Although the preferred embodiment handling the encrypting of data as described above, one of ordinary skill in the art will understand that other methods of encrypting data may be used without departing from the spirit and scope of the present invention.

An additional feature which may be provided with the method in accordance with the present invention is to allow the remote user 106 to request a certain sensitivity level for the current session, or "session sensitivity level". The session sensitivity level must be at or below the remote user's assigned clearance level. This may be useful in certain situations,

such as when the remote user 106 is using a public terminal and do not wish any data above a certain sensitivity level to be downloaded into the public terminal.

Figure 4 is a flowchart illustrating the method for dynamically configuring an encryption strength for data in accordance with the present invention, with the remote user requesting a session sensitivity level. First, the remote user 106 sends identification data and requests a session sensitivity level, via step 402. Next, the remote user's identification data is authenticated, and the session sensitivity level is validated, via step 404. The session sensitivity level is valid if the remote user's clearance allows him to access data with sensitivity levels at or below the requested session sensitivity level. If the remote user 106 is not authenticated or the session sensitivity level is not valid, via step 406, then access to data in the system 100 is denied, via step 408. If the remote user 106 is authenticated and the session sensitivity level is valid, via step 406, then it is determined which pieces of data to which the remote user 106 has clearance to access and which has the requested session sensitivity level or below, via step 410. The encryption strength for the pieces of data is then selected based on the session sensitivity level, via step 412. The cipher suites for each session sensitivity level can be assigned in the same manner as for the clearance level, described above. Other methods for assigning the cipher suites for the session sensitivity levels can also be used without departing from the spirit and scope of the present invention. Once the cipher suite for the session sensitivity level is selected, the pieces of data are encrypted, via step 414. The remote user 106 is then provided access to the encrypted pieces of data, via step 416.

Another feature which may be added to the method for dynamically configuring an

encryption strength for data in accordance with the present invention is allowing other facts to be considered in selecting the encryption strength. For example, the security rating of the output line onto which the data will be provided to the remote user 106 may be taken into account in selecting the encryption strength or cipher suite for a particular clearance or session sensitivity level. For example, data that is to be sent over the Internet, or some other public medium, is to be assigned a stronger encryption than data that is to be sent over a leased line, or some other non-public medium. Similarly, data that is to be sent over a leased line, or some other non-public but non-physically-protected medium, is assigned a stronger encryption than data that is to be sent to another host on the same local area network, or some other physically-protected medium.

Another factor is the sensitivity level of the requested data. For performance enhancement, low-sensitivity data can be encrypted with weaker (faster) encryption even if the remote user has a higher clearance level. Other factors may be considered in the method in accordance with the present invention without departing from the spirit and scope of the present invention.

Any combination of these factors may be considered in selecting the encryption strength. In the preferred embodiment, the degree to which each of these factors is taken into consideration may be configuration by the local user 108.

Although the preferred embodiment selects the encryption strength as described above, one of ordinary skill in the art will understand that other methods of selecting the encryption strength may be used without departing from the spirit and scope of the present invention.

A method for dynamically configuring an encryption strength for data has been disclosed. The method provides remote users with varying levels of clearance to access data. Data in the system is assigned varying sensitivity levels. Each level of clearance allows the remote user to access data of a certain sensitivity level or below. The remote user is assigned a clearance level by the local user. Before the data is provided to the remote user, it is encrypted. The strength of the encryption of the data is based upon the remote user's clearance level or a requested session sensitivity level. In this manner, access control to data is more flexible.

Although the present invention has been described in accordance with the embodiments shown, one of ordinary skill in the art will readily recognize that there could be variations to the embodiments and those variations would be within the spirit and scope of the present invention. Accordingly, many modifications may be made by one of ordinary skill in the art without departing from the spirit and scope of the appended claims.